Information Technology (IT) Access Control Standard

Issue Date: June 1, 2004
Effective Date: June 1, 2004

Number: HHSS-2004-002-C

1.0 Purpose

Access to information technology (IT) resources is critical for HHSS staff, contractors, and business partners to effectively perform their job duties.

Securing and protecting HHSS IT resources is a critical responsibility of every individual with access to HHSS IT resources. Failure to be vigilant by any one individual puts everyone at risk.

This standard establishes guidelines for creation of Unique User Identification (also referred to as Log-on ID) and Strong Password access controls, and the protection of these access controls. It's sole purpose is to ensure the security of the tools critical in providing HHSS services.

2.0 Scope

The scope of this standard applies to all HHSS personnel, contractors, vendors and business partners with access to HHSS IT resources. The standard applies to all access into the HHSS network or any system owned, leased, or supported by HHSS that stores protected HHSS information.

3.0 Standard

This standard provides guidelines for compliance to the IT Security Policy No. HHSS-2004-002.

Security Safeguards covered under this standard apply to Unique User Identification and Password Management. It is the responsibility of all individuals authorized to access HHSS IT resource to follow all access control standards to secure Log-on IDs, Passwords, and other access control safeguards as defined below.

Creation, use, and maintenance of HHSS assigned Unique User Identification and Passwords must meet the requirements detailed in the guidelines below.

With the diversity of IT systems and software applications employed by HHSS, safeguards must be implemented to meet State and Federal security and privacy regulations. This standard is designed to meet safeguard rules which require access to IT resources be uniquely identified and activity tracked while accessing HHSS IT resources.

The following requirements are minimum standards for HHSS IT Resources. If an HHSS business area requires stricter standards, those requirements must be reviewed and approved by Information Systems & Technology (IS&T). It is the responsibility of the business areas to inform and train their staff regarding rules exceeding those set down in this standard.

3.1 Unique User Identification Guidelines

Unique User Identification (Log-on ID) is used to identify an individual, provide services, and levels of access to HHSS networks and applications. Some of the more common uses include LAN access, web accounts, e-mail accounts, screen saver protection, and role based access levels to application functionality and information.

Unique identifiers are used as safeguards to monitor and audit appropriate access and to protect an individual's access from unauthorized intrusion.

Log-on IDs Guidelines

- Every individual accessing a HHSS production IT Resource must have a unique Log-on ID assigned to them by IS&T. No generic or sharing of Log-on IDs is allowed. Use of or sharing a Log-on ID not specifically assigned to the individual is a violation of this standard.
- The HHSS Supervisor or Business Area Administrator is responsible for requesting access on behalf of their staff, contractors, vendor, or business partners through designated HHSS Security Administrators. Each request must include system, applications, and level of access being requested.
- The HHSS Supervisor or Business Area Administrator is responsible for appropriate use and management of all Log-on IDs assigned to staff, contractors, vendors, and business partners managed or contracted by them. All changes or terminations associated with the individual of a Log-on ID assigned to them, must be reported through their Security Administrator immediately.
- Special Log-on IDs requested to meet unique requirements, (i.e., mainframe batch job processing, system maintenance requirements, training IDs) must be approved by the HHSS IT Security Administrator.
    - When special Log-on IDs are created, they must be assigned to an HHSS employee who is directly responsible and will be held accountable for any and all activity preformed using the Log-on ID.
    - All special Log-on IDs must be terminated immediately when no longer needed.
    - Special Log-on IDs must be terminated or reassigned when the responsible HHSS employee terminates or transfers.
- Any Log-On ID not used within the last 180 days may be automatically inactivated without notification to the individual owner. Any Log-on ID not used within a 12 month period will be automatically deleted.

3.1.1 Log-on ID Protection Guidelines

It is the responsibility of the Log-on ID owner to protect the integrity of the Log-on ID assigned to them. Log-on ID owners must comply with the following protection standards:

- Only authorized Security Administrators or HHSS Help Desk Security Administrators may assign or make changes to Log-on IDs.
- Where possible, don't use the same Log-on ID for various HHSS access needs. For example, select one Log-on ID for the LAN Access and a separate Log-on ID for Lotus Notes systems.
- Do not share HHSS Log-on IDs with anyone **INCLUDING SUPERVISORS, administrative assistants, co-workers, or staff assistants**. All Log-on IDs are to be treated as **SENSITIVE, CONFIDENTIAL** HHSS information. Supervisors or managers that require access to a staff member, contractor, vendor, or business partner account must contact the HHSS Help Desk for assistance.
- Do not reveal a Log-on ID over the telephone or through an e-mail message. There should be no legitimate need to reveal your Log-on ID over the telephone or through an e-mail request. Should support staff (Help Desk and Hardware Technicians) need access to assist you with a problem, there are procedures which monitor their activity.
- Do not reveal a Log-on ID in an unsecured e-mail message.
- Do not talk about a Log-on ID in front of others.
- Do not reveal a Log-on ID on questionnaires or security forms.
- Do not share a Log-on ID with family members.
- Do not reveal a Log-on ID to co-workers while on vacation.

- Do not write Log-on IDs down and store them anywhere in your office where they may be lost, stolen, or otherwise compromised. Do not store Log-on IDs in a file on ANY computer system (including a PDA or similar devices) without encryption.
- If you suspect an account or Log-on ID has been compromised, report the incident to the HHSS Help Desk as soon as possible.

3.1.2 Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Must support and enforce the minimum Log-on ID guidelines detailed in this document.
- Must support authentication of individual users, not groups.
- Should provide for access level management based upon a role assigned to a Log-on ID.

3.2 General Password Guidelines

Passwords are an important aspect of computer security and are the front line of protection for log-on ID accounts. Passwords are used for various purposes at HHSS i.e. LAN access, web accounts, e-mail accounts, screen saver protection, and user level application access.

A poorly chosen password may result in the compromise of the HHSS network. As such, all HHSS employees (including contractors, vendors, and business partners with access to HHSS systems) are responsible for taking the appropriate steps, as outlined in this standard, to select and secure passwords. Password owners are responsible for any action or activity performed using their password.

This standard establishes guidelines for creation of strong passwords, the protection of those passwords, and the frequency for changing passwords.

Due to the diversity of HHSS applications, the password standard is divided into two sets of guidelines. The first set applies to all HHSS applications that run on the state mainframe computer utilizing mainframe security safeguards (this includes N-FOCUS, CHARTS, MMIS, C1, C5, and CMS). The state mainframe safeguards are defined and managed by the IMServices, a division of DAS (Department of Administrative Servcies) and are outside the control of HHSS. The systems listed above will employ the mainframe password standard listed in this document. All other HHSS IT resources and applications must meet the Network/Application password guidelines defined in this document.

Mainframe Passwords Guidelines:

- Mainframe strong passwords are to consist at a minimum of six (6) and maximum of eight (8) characters in a combination of alpha, numeric, and special characters. Combination to consist of:
    - At least one alpha character (a-z,)
    - At least one numeric value (0-9)
    - May include special characters (#$@)
- Password must be changed at least every 90 days. Users may change passwords more frequently to further strengthen their security. The recommended RACF password change interval is every 31 days.
- Passwords cannot be reused for 12 months.
- Log-on ID accounts will be automatically revoked after 3 consecutive unsuccessful password attempts.

Network/Application Password Guidelines:

- Strong passwords are to consist at a minimum of eight (8) characters in a combination containing three (3) of the following four (4) characteristics.
    - At least one UPPER CASE alpha character (A-Z)
    - At least one lower case alpha character (a-z)
    - At least one Numeric value (0-9)
    - At least one special character (~!@#$%^&*()_+-=<>?;’:\)
- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed every 180 days.
- All user-level passwords (e.g., e-mail, LAN access, application access, web, desktop computer, etc.) must be changed at least every 180 days. Users may change passwords more frequently to further strengthen their security. The recommended password change interval is every 90 days.
- Passwords cannot be reused for 12 months.
- Log-on ID accounts will be automatically revoked after 3 consecutive unsuccessful password attempts.

3.2.1 Password Protection Guidelines

It is the responsibility of the password owner to protect the integrity of the password assigned to them. Password owners must comply with the following protection standards:

- Only authorized Security Administrators or HHSS Help Desk Security Administrators may request password resets.
- Do not use the same password for HHSS accounts as for other non-HHSS access (e.g., personal ISP account, e-mail, benefits, etc.).
- Where possible, don't use the same password for various HHSS access needs. For example, select one password for the LAN Access and a separate password for application access.
- Do not share HHSS passwords with anyone **INCLUDING SUPERVISORS**, **administrative assistants, co-workers, or staff assistants**. All passwords are to be treated as **SENSITIVE, CONFIDENTIAL** HHSS information. Should supervisors or managers require access to a staff member account they must contact the HHSS Help Desk for assistance.
- Do not reveal a password over the phone. The only exception would be to Help Desk staff or Hardware Technicians working on a support issue that you initiated. Immediately after resolution of the incident, you must change the password shared with support staff.
- Do not reveal a password in an unsecured e-mail message.
- Do not talk about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaires or security forms.
- Do not share a password with family members.
- Do not reveal a password to co-workers while on vacation.
- If anyone demands a password, refer him or her to this document or have them call the HHSS Help Desk.
- Do not use the "Remember Password" feature of applications.
- Do not write passwords down and store them anywhere in your office where they may be lost, stolen, or otherwise compromised. Do not store passwords in a file on ANY computer system (including a PDA or similar devices) without encryption.
- Change passwords as required by individual applications.
- If you suspect an account or password has been compromised, immediately change the password and report the incident to the HHSS Help Desk as soon as possible.

3.2.2 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

- Must support and enforce the minimum password guidelines detailed in this document.
- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- RACF passwords – Applications using RACF must meet the strongest password guidelines in force and supported by IMServices.

4.0 Enforcement

Log-on ID and Password audits, may be used by IS&T periodically to monitor appropriate use of IT Resources and insure they meet the guidelines set in this standard.

Should a violation of this IT Security Standard occur, the individual(s) who committed the violation will be personally liable for their actions or the actions taken by others due to their violation of this standard. Lack of knowledge of or familiarity with this policy shall not release an individual from such liability. Any employee found to have violated this policy may be subject to disciplinary action, as defined in the governing policy HHSS 2004-002

5.0 Revision History

HR Legal – 03/12/2004

CCT Approval – 05/27/2004